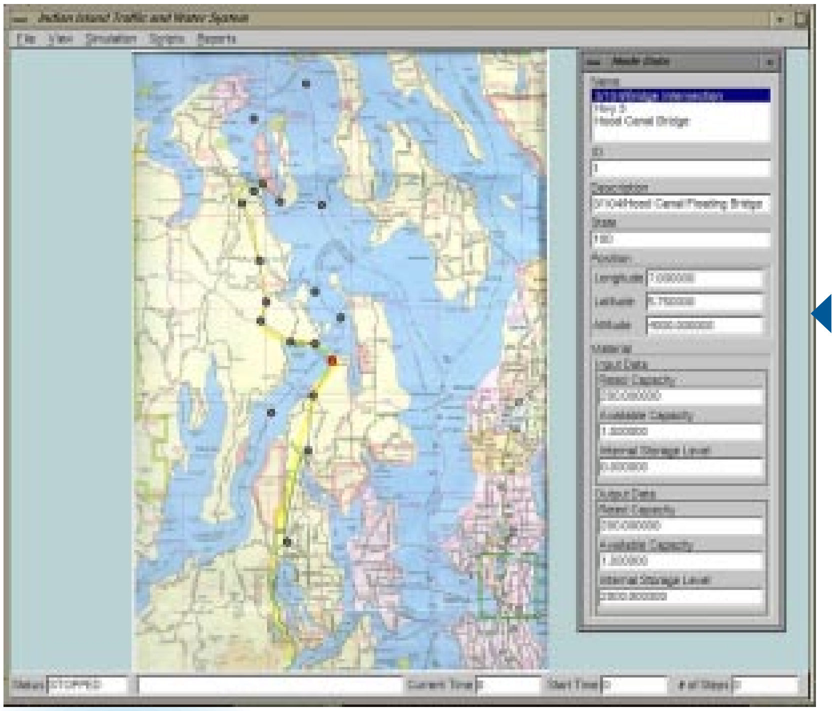
INEEL NATIONAL SECURITY

War Gaming for the Real World



Indian Island Traffic and Water System

Name: 3/13 Windage Intersection, Hwy 3, Hood Canal Bridge

ID: 1

Description: 3/104/Hood Canal Floating Bridge

State: TBD

Position: Longitude 7.000000; Latitude 5.750000; Altitude 4000.000000

Material

Input Data: Rated Capacity 2800.000000; Available Capacity 1.000000; Internal Storage Level 0.000000

Output Data: Rated Capacity 2800.000000; Available Capacity 1.000000; Internal Storage Level 2800.000000

Status: STOPPED; Current Time: 0; Start Time: 0; # of Steps: 0

The INEEL is developing a modeling and simulation tool that offers high user interaction in a war-gaming environment. CIMS allows a user to rapidly construct and evaluate infrastructure models.

Idaho National Engineering and Environmental Laboratory

Critical Infrastructure Modeling Systems (CIMS)

Protecting and recovering from attack

The Problem

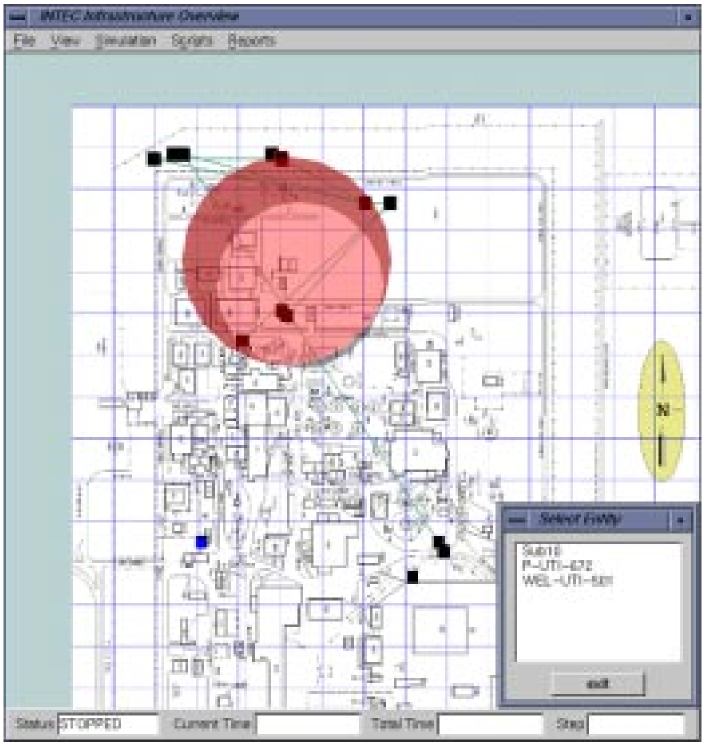
Critical infrastructures are complex physical and cyber-based systems essential to the minimum operations of the economy and government, including transportation, telecommunications, energy, banking and finance, water systems, and emergency services.

Infrastructures have become increasingly automated and interlinked. Modern commercial infrastructures are composed of a collection of interconnected networks serving different purposes with different owners. Deliberate attacks or accidental system failure may result in serious consequences to multiple infrastructures affecting the region—even the nation. Government and industry do not have methods to identify what portions of their infrastructure is the minimum critical subnetwork necessary to perform their mission or how to best handle their assets to preserve their mission.

The Solution

INEEL is developing a computer model to quickly identify the portions of critical infrastructure necessary to maintain an essential mission when that infrastructure is attacked by a knowledgeable and capable adversary. The model will:

Continued on back



Status: STOPPED

Select Entity:
Sub10
P-UTI-672
WEL-UTI-521

Continued from front

- Identify critical portions of multiple infrastructures for defined missions.
- Identify vulnerabilities and interdependencies of critical nodes/lines/ components.
- Analyze capacities and alternatives when portions of infrastructure are unavailable.
- Detect and identify what portion of infrastructure is being attacked.
- Prioritize remediation and hardening assets.

Project Description and Approach

The INEEL is developing an algorithmic process for remediation of critical and vulnerable assets of a critical infrastructure, including its unstressed performance, and its emergent behavior when under attack.

These methods will determine the smallest part of an infrastructure that can still execute its critical function and will prioritize and analyze critical nodes/lines/components and will assess what channels are available in the event of a deliberate attack, the capacity of those alternate channels, and the priority of the flow if the channel limits the normal amount of transmission.

The process will model emergent behaviors, which could include detecting when, or if your distribution network is being attacked, and decision-making tools for quick recovery reconfiguration of a system after successful attack on a critical subnetwork.

The INEEL will develop approaches and methodologies to prioritize deployment of limited remediation resources when the simulation of these emergent behaviors finds assets that are both critical and vulnerable to a knowledgeable adversary.

Model Approach

The most important feature of the model-generation process is the matching of the survivability requirements and objectives with a graph and scheduling model. Model generation translates the critical infrastructure into a task graph with applicable specifications, augmented with mechanisms to facilitate task interdependence. A scheduling model is derived. Dynamic behavior of the models considers changes to the size of the graph, dependencies, priorities and optimization criteria. Further consideration may include adaptability. The approach will use existing algorithms and complexity analysis tools used in general graph and scheduling theory.

Once critical subnetworks are identified, their behavior can be simulated. Simulations of attack scenarios/failures will define the compromised portions of the infrastructure. In addition, the program develops heuristic algorithms to find essential points for “hardening”, which can save significant portions of the network from a particular attack scenario or a bundle of attack scenarios.

Point of Contact:

Ken Watts
208-526-9628
kdw@inel.gov

Don Dudenhoeffer
208-526-0700
dudedd@inel.gov